RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: IMT-R02

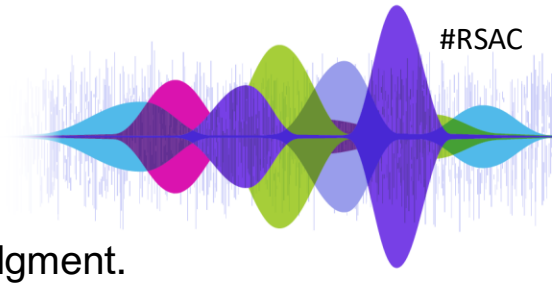
Forensic Investigative and Legal Challenges with New Cyber Regulations

MODERATOR: **Jacqueline "Lyn" Brown**
Partner, Privacy, Cyber & Data Governance
Wiley Rein, LLP
https://www.linkedin.com/in/lyn-brown

PANELISTS: **Erin Joe**
Cybersecurity Executive
https://www.linkedin.com/in/erin-joe/

Michael Machtinger
Section Chief, Cyber Division
Federal Bureau of Investigation (FBI)
linkedin.com/in/mikemachtinger

Jennifer Burnside
Practice Lead, Cyber Crisis Communications
Mandiant | Google Cloud
https://www.linkedin.com/in/jennifer-starling-burnside/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rig hts reserved.

For Google, case studies and examples are drawn from our experiences and activities working for a variety of customers and does not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals.

The material contained in this presentation from Wiley Rein LLP is for informational purposes only. It is not intended to be and is not considered to be legal advice. Legal advice of any nature should be sought from legal counsel.

The moderator and panelists are providing their personal opinions and experience as current or former FBI employees and not the official position of the federal government.

RSAC | 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Lyn Brown

Wiley Rein LLP
https://www.linkedin.com/in/lyn-brown

PANELISTS:

Erin Joe

Cybersecurity Executive
linkedin.com/in/erin-joe

Michael Machtinger

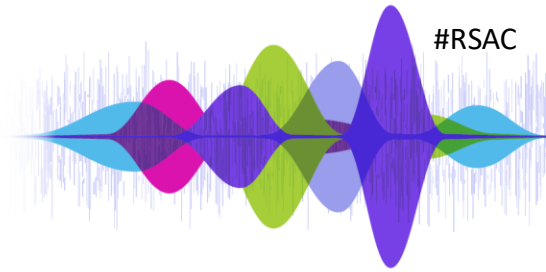
Federal Bureau of Investigation (FBI)
linkedin.com/in/mikemachtinger

Jennifer Burnside

Mandiant | Google Cloud
linkedin.com/in/jennifer-starling-burnside

wiley | Google Cloud Security

Cyber Incident Reporting Requirements



Securities and Exchange Commission	Department of Defense (DFARS 7012)	Cybersecurity and Infrastructure Security Agency (proposed)
➢ Public companies must disclose "material cybersecurity incidents" within 4 business days of discovery.	➢ Contractors must "rapidly report" a "cyber incident" within 72 hours of discovery.	➢ Critical infrastructure entities must report cyber incidents within 72 hours for "covered cyber incidents"; must report ransom payments within 24 hours.

LEGAL PRIVILEGES

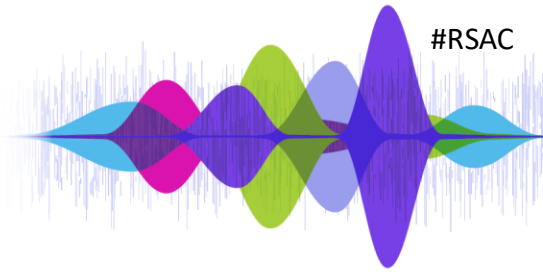
Attorney Client Communications

- Applies to communications.
- Between a lawyer and client.
- For the purpose of seeking legal advice.
- Privilege can be waived by intentional disclosure to a third party.

Attorney Work Product

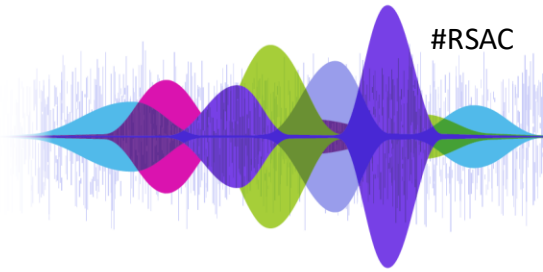
- Applies to documents and tangible things.
- Prepared in anticipation of litigation or trial.
- Prepared by or for a party or their representative.

Privileged communications and work product may not be subject to disclosure in litigation.



In Re Rutter's Data Security Breach Litigation

- Company retained outside counsel the same day it received security alerts for advice on "potential notification obligations."
- Outside counsel retained forensic firm the next day "to determine whether unauthorized activity … resulted in the compromise of sensitive data…."
- Litigation was not contemplated when forensic report prepared.
- Report/related communications were not protected by privilege:
  - Report was prepared in the "ordinary course" and discussed facts;
  - Primary purpose of the report was not to assist in providing legal advice.



In Re Target Corp. Customer Data Security Breach Litigation

- Two-track investigative approach:
  - "Ordinary course" investigation for non-privileged review;
  - Data Breach Task Force under privilege for legal advice.
- Target demonstrated that the Data Breach Task Force was not focused on remediation but on informing in-house and outside counsel so they could provide legal advice and prepare for litigation.
- Target also produced documents/tangible things, including forensic images, that allowed plaintiffs to learn how the data breach occurred from a separate report not engaged by counsel.

APPLY – LESSONS LEARNED

CHALLENGES

- Tight reporting deadlines.
- Divergent views of materiality.
- Stakeholder tensions.
- Potential for data breach litigation.
- Difficulties with protecting privilege.

BEST PRACTICES

- Adopt a proactive and multi-layered approach to minimize risk.
- Preparation and collaboration are key.
- Establish a relationship with the FBI before a critical incident.
- Consider implications of a dual track forensic investigation under privilege.
- Engage outside counsel, forensic firms, crisis communications under privilege.
- Understand reporting obligations and timelines in advance.

RSAC™ 2025 Conference

Many Voices.
One Community.

Lyn Brown

Partner,
Privacy & Cyber

Wiley Rein, LLP

Erin Joe

Senior Executive,
Cybersecurity

Michael Machtinger

Section Chief, Cyber Division

Federal Bureau of Investigation

Jennifer Burnside

Practice Lead, Crisis Communications

Google Cloud/Mandiant